REPORT DOCUMENTATION PAGE	Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY) 04-12-2018	2. REPORT TYPE Final Report	3. DATES COVERED (From - To) 15-Sep-2017 - 14-Sep-2018

4. TITLE AND SUBTITLE Final Report: Research, Education and Workforce Training for Engagement in the Cyber-learning Environment	5a. CONTRACT NUMBER W911NF-17-1-0556
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER 106012
6. AUTHORS	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES Florida International University 10555 West Flagler, EC 2441 Miami, FL 33174 -1630	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES) U.S. Army Research Office P.O. Box 12211 Research Triangle Park, NC 27709-2211	10. SPONSOR/MONITOR'S ACRONYM(S) ARO 11. SPONSOR/MONITOR'S REPORT NUMBER(S) 70457-CS-REP.1

12. DISTRIBUTION AVAILIBILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON Sitharama Iyengar
a. REPORT UU	b. ABSTRACT UU	c. THIS PAGE UU	UU		19b. TELEPHONE NUMBER 305-348-3947

RPPR Final Report
as of 24-Jan-2019

Agency Code:

Proposal Number: 70457CSREP **Agreement Number: W911NF-17-1-0556**

INVESTIGATOR(S):

Name: Leonardo Bobadilla
Email: bobadilla@cs.fiu.edu
Phone Number: 3053482744
Principal: N

Name: Bogdan Carbunar
Email: carbunar@cs.fiu.edu
Phone Number: 3053487566
Principal: N

Name: Ph.D. Sitharama S Iyengar
Email: iyengar@cis.fiu.edu
Phone Number: 3053483947
Principal: Y

Name: Michael Robinson
Email: michael.robinson13@fiu.edu
Phone Number: 3053482744
Principal: N

Name: M.S. Jerry Miller
Email: millej@fiu.edu
Phone Number: 3053483751
Principal: N

Name: Deng Pan
Email: pand@cs.fiu.edu
Phone Number: 3053487567
Principal: N

Name: Niki Pissinou Ph.D.
Email: pissinou@fiu.edu
Phone Number: 3053483716
Principal: N

Name: Ruogu Fang
Email: rfang@cs.fiu.edu
Phone Number: 3053487982
Principal: N

Organization: **Florida International University**
Address: 10555 West Flagler, EC 2441, Miami, FL 331741630
Country: USA
DUNS Number: 071298814 EIN: 756000121
Report Date: 14-Dec-2018 Date Received: 04-Dec-2018
Final Report for Period Beginning 15-Sep-2017 and Ending 14-Sep-2018
Title: Research, Education and Workforce Training for Engagement in the Cyber-learning Environment
Begin Performance Period: 15-Sep-2017 **End Performance Period:** 14-Sep-2018
Report Term: 0-Other
Submitted By: M.S. Jerry Miller Email: millej@fiu.edu
Phone: (305) 348-3751
Distribution Statement: 1-Approved for public release; distribution is unlimited.

STEM Degrees: 19 **STEM Participants:** 49

Major Goals: The goal of this equipment purchase was to enhance our cyber security programs in penetration testing, digital forensics, biometric sciences, identity science, and security in the areas of cloud computing, and big data analysis, as well as security of deployed sensor systems. The FIU School of Computing and Information Sciences Labs in the College of Engineering and Computing laboratories did not have any hardware dedicated to these areas; this is particularly limiting since we need systems segregated from the University's existing networks to fully enable our cyber security research programs.
The areas of research and cybersecurity targeted were;
1. Fraud and Malware Detection in Social Media
2. Research and Education in STEM, particularly in cybersecurity, deep learning/AI, and social media technologies
3. Computer Hardware and Digital Logic Labs/Research
4. Penetration testing and digital forensics
5. Network flow/security through 3-D application in Integrated Computer Augmented Virtual Environment (I-CAVE)
Institutes/Centers/Labs benefiting from the new equipment were;
Telecommunications and Information Technology (IT2) Institute,
Center for Cyber Infrastructure Education and Research for Trust and Assurance (CIERTA)
Cybersecurity and Privacy Research (CaSPER) Lab
SCIS Hardware Lab
The Integrated Computer Augmented Virtual Environment (I-CAVE)

Accomplishments: Equipment was purchased and installed in accordance with the approved grant, including the following items or their suitable substitutes as approved.:
(1) Rackform R4552.v6 with 3xGPUs,
(2) nine Dell PowerEdge R430 Servers with 8SFF Advanced SATA,
(3) two HP 5900AF-48G 4XG-2QSFP+switches, (4) two Rackform U623.v6 Research Systems with GPUs,
(5) a single Rackform U623.v6 (without GPU) Research Systems,
(6) Arista 7150S-52x10GbE (SFP+) Switch Research System, and
(7) ARISTA 7280QR with 24x40GbE+1, 2x100GbE (SFP+) Switch Research Network.
As a result, the following project sections were improved;
The CIERTA and associated labs at FIU School of Computing and Information Sciences, including;
Cyber security programs in penetration testing,
Digital forensics,
Biometric sciences,
Identity science,
Game theoretic security in the areas of cloud computing, big data analysis and security, as well as
Security of deployed sensor systems and sensor data cleaning and associated Artificial intelligence (AI),
Augmented Reality /Virtual Reality (ICAVE) programs. .

RPPR Final Report

as of 24-Jan-2019

Training Opportunities: As the equipment was purchased and installed throughout the year, the following programs were able to use the equipment for student training.

1. Cybersecurity and Privacy Research (CaSPER) Lab Camera Based Two-Factor Mobile and Wearable Authentication. We have introduced Pixie, a novel, camera based two factor authentication solution for mobile and wearable devices. Pixie leverages a quick and familiar user action of snapping a photo to simultaneously perform a graphical password authentication and a physical token-based authentication. However, Pixie does not require expensive, uncommon hardware. Pixie establishes trust based on both the knowledge and possession of an arbitrary physical object readily accessible to the user, called ``trinket''. Users choose their trinkets similar to setting a password and authenticate by presenting the same trinket to the camera. The fact that the object is the trinket, is secret to the user.
In addition, We have used our GPU server to implement ai.lock in Android using Tensorflow and show that it is resilient to attacks. Specifically, we have captured, collected and generated datasets of 250,332 images, and generated 1 million synthetic credentials. We have used these datasets to generate attack datasets containing more than 3.5 billion (3,567,458,830) authentication instances. We have shown on 140 million synthetic image attack samples, ai.lock had a false accept rate (FAR) of 0.2×10-6 %. We have shown that ai.lock was unbreakable when tested with 1.4 billion synthetic credential attack samples. We estimated the Shannon entropy of ai.lock on 2 billion image pairs to be 18.02 bits, comparing favorably with state-of-the-art biometric solutions. Further, we have shown that ai.lock is a delta-LSIM function, over images that we collected. ai.lock is fast, imposing an overhead of under 1s on a Nexus 6P device.
Student participants from this lab included;

a. 1 female graduate student and
b. 1 minority undergraduate student.
c. 3 other graduate students.

SCIS Hardware Lab used the new equipment to conduct the following training, in addition to the proposed uses;

- Cyber Security Software and Hardware training
- Create Virtual Machines that are White, Gray and Black hat targets for our local students.
- Create Virtual Machines that are White, Gray and Black hat targets to be used by other FIU students, including Dual Enrollment
- Create Virtual Machines that are White, Gray and Black hat targets to be used by High Schools

The following projects were also conducted as a result of the equipment;

- Cyber Security Intranet Network project
- Wireless (4) used for Cyber Security
- Capture the Flag Competitions
- IDS 3917 Hardware and Software Cyber Class (21 students Spring 2018)
- Cyber Security Level 1 Training leading towards CEH (Certified Ethical Hacker) Certification
- Cyber Security Level 2 Training leading towards CEH (Certified Ethical Hacker) Certification
- Creating automatic Virtual OS loading from Server Host into client Virtual machines, so that students can log in and obtain multiple machines to be penetrated

As a result, student diversity was enhanced and training was completed on the following minority group students;

1. Nine Hispanic students
2. Four Asian students

Through this course, and other research work using the equipment, 14 undergraduate students and 3 graduate students received degrees just this past year.
More importantly,we have been able to place the following students in the workforce; 10 + DoD

1	NSA
1	CIA
1	Pentagon
3	CyberArk/Israeli Cyber Security Company
1	Microsoft
1	Private School System in Broward County
1	Private Company in Miami
1	Private company in California/Chicago

1	Home Depot
1	Wells Fargo
1	Baptist Hospital

Results Dissemination: Installation and use of the equipment has been disseminated as an acknowledgement for US Army Research Office funding/research support on 26 student/professional poster presentations.

In addition, any future research papers, several of which are currently being written, will be acknowledging US Army Research Office funding/research support.

Honors and Awards: Nothing to Report

Protocol Activity Status:

Technology Transfer: Nothing to Report

Summary of research projects on which equipment has been or will be used for

Telecommunications and Information Technology (IT2) Institute

Center for Cyber Infrastructure Education and Research for Trust and Assurance (CIERTA)

Cybersecurity and Privacy Research (CaSPER) Lab

SCIS Hardware Lab

The Integrated Computer Augmented Virtual Environment (I-CAVE)

Cybersecurity and Privacy Research (CaSPER) Lab Camera Based Two-Factor Mobile and Wearable Authentication. We have introduced Pixie, a novel, camera based two factor authentication solution for mobile and wearable devices. Pixie leverages a quick and familiar user action of snapping a photo to simultaneously perform a graphical password authentication and a physical token-based authentication. However, Pixie does not require expensive, uncommon hardware. Pixie establishes trust based on both the knowledge and possession of an arbitrary physical object readily accessible to the user, called ``trinket''. Users choose their trinkets similar to setting a password and authenticate by presenting the same trinket to the camera. The fact that the object is the trinket, is secret to the user.

We have developed robust, novel features from trinket images, and leveraged supervised learning classifiers to effectively address inconsistencies between images of the same trinket captured in different circumstances. Further, in order to help the users pick high quality trinkets and images thereof, we have developed features that capture the quality of reference images as defined by the likelihood of causing false accepts or false rejects during authentication. We have used these features to train a trinket image rejection classifier that detects low quality images before they can be used as Pixie trinkets. In addition, to provide meaningful actionable feedback, we have identified feature threshold values that pinpoint problem images and naturally translate them into user instructions.

We have introduced several image-based attacks, including an image-based dictionary (or ``pictionary'') attack. Pixie achieved a FAR below 0.09% on such an attack consisting of 14.3 million authentication attempts constructed using public trinket image datasets and images that we collected online. We have shown that Pixie is resilient to a shoulder surfing attack flavor where the adversary knows or guesses the victim's trinket object type. Specifically, on a targeted attack dataset of 7,853 images, the average number of ``trials until success'' exceeds 5,500 irrespective of whether the adversary knows the trinket type or not. In addition, we introduced and studied the concept of ``master images'', whose diverse keypoints enable them to match multiple trinkets. We have developed features that enable Pixie to reduce the effectiveness of master images.

We have also performed a user study with 42 participants over 8 days in 3 sessions and have shown that Pixie is discoverable: without prior training and given no external help, 86% and 78% of the participants were able to correctly set a trinket then authenticate with it, respectively. Pixie's trinkets were perceived as more memorable than text passwords and were also easily remembered 2 and 7 days after being set.

ai.lock: A Secure Mobile Authentication Alternative to Biometrics. To ensure Pixie's resilience to candidate images captured in different circumstances than the reference images, we leveraged a statistical classifier using features which exploit robust key points extracted from the trinket images. However, this approach raises new challenges. First, an adversary who captures or compromises the device that stores the user's reference credentials (e.g. mobile device, remote server) and has access to its storage, should not be able to learn information about the reference credentials or their features. Second, while biometric features such as ridge flow of fingerprints or eye socket contours of faces, can be captured with engineered features and are invariant for a given user, images of objects and general scenes lack a well-defined set of features that can be accurately used for authentication purposes.

To address these challenges, we have developed ai.lock, a practical, secure and efficient image based authentication system that converts general mobile device captured images into biometric-like structures, to be used in conjunction with secure sketch constructs and provide secure authentication and storage of credentials. To extract invariant features for image based authentication, ai.lock leverages (1) the ability of Deep Neural Networks (DNNs) to learn representations of the input space (i.e., embedding vectors of images) that re.ect the salient underlying explanatory factors of the data, (2) Principal Component Analysis (PCA) to identify more distinguishing components of the embedding vectors and (3) Locality Sensitive Hashing (LSH) to map the resulting components to binary space, while preserving similarity properties in the input space. We call the resulting binary values imageprints. ai.lock builds on a secure sketch variant to securely store reference imageprints and match them to candidate imageprints. Further, we proposed the LSH-inspired notion of locality sensitive image mapping functions, that convert images to binary strings that preserve the "similarity" relationships of the input space, for a desired similarity definition.

In addition, we have developed brute force image based attacks that aim to defeat ai.lock. First, we introduced real image attacks, that use manually collected and publicly available image datasets. To evaluate ai.lock on large scale attack images, we introduced synthetic image attacks that use images produced by generative models. To evaluate the resilience of stored credentials, we introduce synthetic credential attacks, that use authentication credentials generated with the same distribution of the credentials extracted from manually collected images.

We have used our GPU server to implement ai.lock in Android using Tensorflow and show that it is resilient to attacks. Specifically, we have captured, collected and generated datasets of 250,332 images, and generated 1 million synthetic credentials. We have used these datasets to generate attack datasets containing more than 3.5 billion (3,567,458,830) authentication instances. We have shown on 140 million synthetic image attack samples, ai.lock had a false accept rate (FAR) of 0.2×10^{-6} %. We have shown that ai.lock was unbreakable when tested with 1.4 billion synthetic credential attack samples. We estimated the Shannon entropy of ai.lock on 2 billion image pairs to be 18.02 bits, comparing favorably with state-of-the-art biometric solutions. Further, we have shown that ai.lock is a delta-LSIM function, over images that we collected. ai.lock is fast, imposing an overhead of under 1s on a Nexus 6P device.

Estimate of number of students (breakout by estimated minority/underrepresented groups who have worked on the equipment

a. 1 female graduate student and
b. 1 minority undergraduate student.
c. 3 other graduate students.

SCIS Hardware Lab
1. Summary of the research projects on which equipment has been or will be used, including support of (a) the research work described in the proposal and

- Cyber Security Software and Hardware training
- Create Virtual Machines that are White, Gray and Black hat targets for our local students.
- Create Virtual Machines that are White, Gray and Black hat targets to be used by other FIU students, including Dual Enrollment
- Create Virtual Machines that are White, Gray and Black hat targets to be used by High Schools

2. Other research work of interest to DoD for which the equipment is being used, and;

- Cyber Security Intranet Network
- Wireless (4) used for Cyber Security
- Capture the Flag Competitions
- IDS 3917 Hardware and Software Cyber Class 21 students Spring 2018
- Cyber Security Level 1 Training leading towards CEH (Certified Ethical Hacker) Certification
- Cyber Security Level 2 Training leading towards CEH (Certified Ethical Hacker) Certification
- Creating automatic Virtual OS loading from Server Host into client Virtual machines, so that students can log in and obtain multiple machines to be penetrated

3. Estimate of number of students (breakout by estimated minority/underrepresented groups who have worked on the equipment
9 Hispanics + ids + present semester
3 Asian
1 Middle Eastern

4. If you have graduated anyone, please also let me know the numbers and

14 Undergraduate
3 Graduate

5. where they may have gone, i.e., 2 students now working in NSA/CIA, Google, Microsoft, etc.:

Some have graduated, some are attending Graduate School
10 + DoD

1	NSA
1	CIA
1	Pentagon
3	CyberArk/Israeli Cyber Security Company
1	Microsoft
1	Private School System in Broward County
1	Private Company in Miami
1	Private company in California/Chicago
1	Home Depot
1	Wells Fargo
1	Baptist Hospital